

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-162965

(43)Date of publication of application : 16.06.2000

(51)Int.Cl.

G09C 1/00

(21)Application number : 10-337108

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 27.11.1998

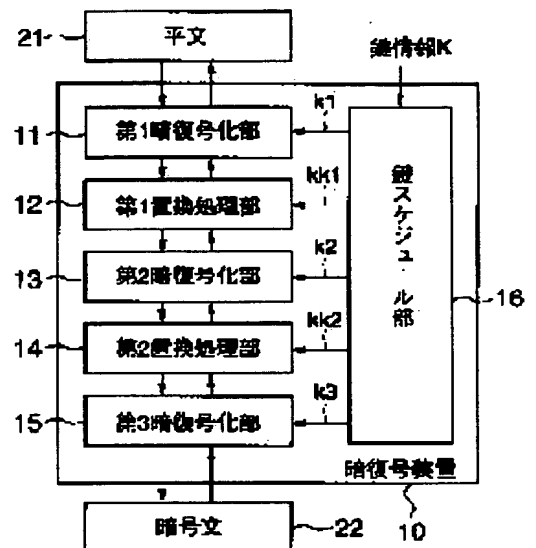
(72)Inventor : SANO FUMIHIKO
KAWAMURA SHINICHI
SHIMIZU HIDEO

(54) CIPHERING AND DECIPHERING DEVICE, AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an algorithm more efficient than a simple three-staged DES-SS and also resistant to a difference attack and a linear attack, although it configures a single encryption algorithm compatible to any of DES, triple DES, and DES-SS.

SOLUTION: This device is a ciphering and deciphering device 10 which ciphers a plain text 21 into a cipher-text 22 and/or decipher a cipher-text into a plain text, and is provided with a 1st ciphering and deciphering means 11 for processing by ciphering or decipher processing, a 1st substituting means 12 for substituting a data for an output of the 1st ciphering and deciphering means according to a substitution table, a 2nd ciphering and deciphering means 13 for processing an output of the 1st substituting means by ciphering or deciphering, a 2nd substituting means 14 for substituting a data for the output of the 2nd ciphering and deciphering means according to a predetermined substitution table, and a 3rd ciphering and deciphering means 15 for ciphering or deciphering an output of the 2nd substituting means.



LEGAL STATUS

[Date of request for examination] 06.02.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3679936

[Date of registration] 20.05.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

13

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-162965

(P2000-162965A)

(43) 公開日 平成12年6月16日 (2000. 6. 16)

(51) Int.Cl.⁷

G 0 9 C 1/00

識別記号

6 1 0

F I

G 0 9 C 1/00

テマコード* (参考)

6 1 0 B 5 J 1 0 4

審査請求 未請求 請求項の数 9 O L (全 14 頁)

(21) 出願番号

特願平10-337108

(22) 出願日

平成10年11月27日 (1998. 11. 27)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 佐野 文彦

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(72) 発明者 川村 信一

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

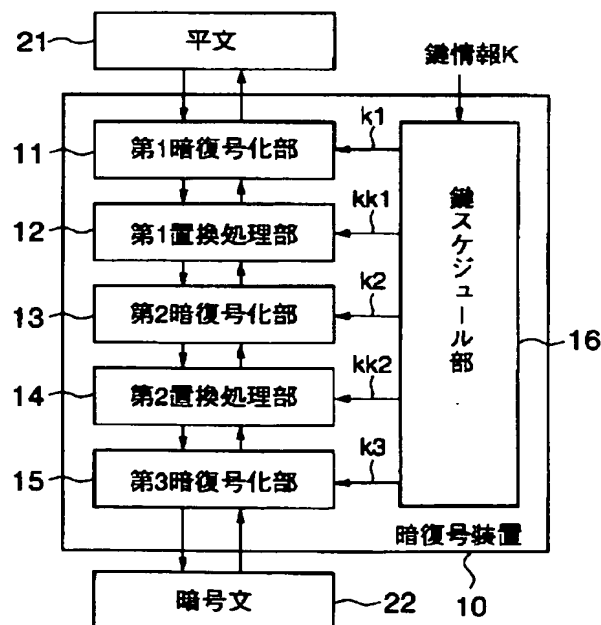
最終頁に続く

(54) 【発明の名称】 暗復号装置及び記憶媒体

(57) 【要約】

【課題】 本発明は、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、単にDES-SSを3段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる。

【解決手段】 平文21を暗号文22に暗号化し、及び又は、暗号文を平文に復号する暗復号装置10であって、暗号処理又は復号処理を行う第1の暗復号化手段11と、第1の暗復号化手段の出力を所定の置換表によりデータ置換する第1の置換手段12と、第1の置換手段の出力に対し、暗号処理又は復号処理を行う第2の暗復号化手段13と、第2の暗復号化手段の出力を所定の置換表によりデータ置換する第2の置換手段14と、第2の置換手段の出力に対し、暗号処理又は復号処理を行う第3の暗復号化手段15とを備えた暗復号装置



【特許請求の範囲】

【請求項 1】 平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置であって、暗号処理又は復号処理を行う第 1 の暗復号化手段と、前記第 1 の暗復号化手段の出力を所定の置換表によりデータ置換する第 1 の置換手段と、前記第 1 の置換手段の出力に対し、暗号処理又は復号処理を行う第 2 の暗復号化手段と、前記第 2 の暗復号化手段の出力を所定の置換表によりデータ置換する第 2 の置換手段と、前記第 2 の置換手段の出力に対し、暗号処理又は復号処理を行う第 3 の暗復号化手段とを備えたことを特徴とする暗復号装置。

【請求項 2】 前記第 1 の暗復号化手段と前記第 3 の暗復号化手段、並びに、前記第 1 の置換手段と前記第 2 の置換手段は、それぞれ同一のアルゴリズムに従う手段となることを特徴とする請求項 1 記載の暗復号装置。

【請求項 3】 前記第 1、第 2 及び第 3 の暗復号化手段並びに前記第 1 及び第 2 の置換手段それぞれに与える中間鍵を生成する鍵生成手段を備えるとともに、前記第 1 及び第 2 の置換手段は、前記鍵生成手段が生成した中間鍵に所定の情報が含まれているときには恒等変換として機能することを特徴とする請求項 1 又は 2 記載の暗復号装置。

【請求項 4】 前記第 1 及び又は第 3 の暗号復号化手段は、前記鍵生成手段が生成した中間鍵に所定の情報が含まれているときには、前記第 2 の暗号復号化手段と同一のアルゴリズムに従う手段となることを特徴とする請求項 3 記載の暗復号装置。

【請求項 5】 前記第 2 の暗復号化手段は、前記第 1 及び第 3 の暗号復号化手段が暗号化処理を行うときには復号処理を実行し、前記第 1 及び第 3 の暗号復号化手段が復号処理を行うときには暗号化処理を実行することを特徴とする請求項 3 又は 4 記載の暗復号装置。

【請求項 6】 前記鍵生成手段は、前記第 1 及び第 3 の暗号復号化手段に同一の中間鍵を与えることを特徴とする請求項 5 記載の暗復号装置。

【請求項 7】 前記鍵生成手段は、前記第 1 及び第 2 の暗号復号化手段、又は、前記第 2 及び第 3 の暗号復号化手段が同一アルゴリズムとなりかつ同一暗復号鍵を使用する結果となる中間鍵を与えることを特徴とする請求項 5 記載の暗復号装置。

【請求項 8】 平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置を制御するプログラムであって、暗号処理又は復号処理を行わせる第 1 の暗復号化手段と、前記第 1 の暗復号化手段の出力を所定の置換表によりデータ置換させる第 1 の置換手段と、前記第 1 の置換手段の出力に対し、暗号処理又は復号処

理を行わせる第 2 の暗復号化手段と、

前記第 2 の暗復号化手段の出力を所定の置換表によりデータ置換させる第 2 の置換手段と、

前記第 2 の置換手段の出力に対し、暗号処理又は復号処理を行わせる第 3 の暗復号化手段とを有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 9】 前記第 1、第 2 及び第 3 の暗復号化手段並びに前記第 1 及び第 2 の置換手段それぞれに与える中間鍵を生成させる鍵生成手段を備えるとともに、

前記第 1 及び第 2 の置換手段を、前記鍵生成手段が生成させた中間鍵に所定の情報が含まれているときには恒等変換として機能させることを特徴とする請求項 8 記載の記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は暗復号装置及び記憶媒体、特に秘密鍵ブロック暗号により情報を暗号化若しくは復号するのに適した暗復号装置及び記憶媒体に関するものである。

【0002】

【従来の技術】近年の計算機通信技術の発達に伴い、種々の情報がデジタル情報として通信され、また蓄積されるようになってきているが、これらの情報についての機密やプライバシーを保護するために情報を暗号化する必要性が増している。このために、従来は主に DES 方式（特開昭 51-108701）を用いることで、情報の暗号を図っている。

【0003】しかしながら、DES 方式（以下、単に DES ともいう）は 1970 年代に設計された暗号アルゴリズムであり現代の技術進歩に対して安全であるとは言えなくなっている。DES に対する解読攻撃方法としては、56 ビットからなる鍵の総当たり探索や総当たり探索より効率のよい差分攻撃（E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of CRYPTOLOGY, Vol. 4, Number 1, 1991）、線形攻撃（松井充, DES 暗号の線形解読法（I）、暗号と情報セキュリティシンポジウム、1993）等が知られている。

【0004】このような状況から既に広く普及している DES 方式を大幅に変更することなく、解読攻撃に対する防御力を強化する試みとして、トリプル DES が知られている。

【0005】トリプル DES は暗号化を行うのに DES を 3 回適用する方式であり、2 つの鍵を使用して、鍵 1 による暗号化、鍵 2 による復号、鍵 1 による暗号化、という手順により暗号化を行うものである。トリプル DES では DES の鍵を 2 つ用いるので個々の鍵は 56 ビットでありながら、実質的な鍵の長さは 112 ビットであ

ると考えることができる。

【0006】しかし、トリプルDESはDESを3回行うため、DESと較べて処理時間が多くかかってしまうという問題点がある。

【0007】一方、DESを強くしようとする異なる試みとして、DES-SS方式（特開平10-116029）が知られている。

【0008】DES-SS方式（以下、単にDES-Sともいう）では、DES内部で使用されている非線型関数であるF関数の他に新たにG関数を用いることで、DESの安全性を高めている。また、DES-SSの処理ではDESと比較するとG関数の処理が増加しているだけなので、トリプルDESと較べて効率がよいという特徴を持つ。

【0009】さらに、トリプルDESとは異なり56ビットの鍵を複数用いるのではなく、1個の鍵自体の長さが112ビットであるため、総当たり攻撃に対してより安全であるという特徴も持っている。

【0010】DESの56ビットの鍵は8ビットのパーティットを含めて64ビットで表される。DES-Sでは、鍵の上位64ビットと下位64ビットが同じ値である場合には、DESと同じ機能を果たす暗号化関数として動作するという他の暗号方式にない特徴がある。これによりDES-SSを有する暗復号装置では、DES互換モードを設けることが可能になる。

【0011】このDES互換モードの原理は、鍵の上位と下位が等しい場合には、G関数の入力と出力が一致する関数、すなわち恒等変換であることに基づいている。DES-SSのもつDES互換モードを利用することにより、1つの暗復号装置で2つの暗号化を行うことができ、装置規模を小さくできるという利点がある。

【0012】

【発明が解決しようとする課題】上記したように、DES、トリプルDES、DES-Sにはそれぞれ長所と短所がある。ここで、情報暗号化の要請及び高強度の必要性がますます高くなっていること、及び、DESは広く普及していること、等の事情を考え合わせれば、DES及びその応用暗号化技術との互換性を確保しつつ強度の高い暗号化も可能な技術を提供することが重要になってきている。

【0013】しかし、この技術の実現にあたっては、暗号の効率性という点も考慮に入れなければならない。

【0014】例えばDES-Sを用いれば、DESより安全でトリプルDESより効率のよい暗号化を行うことができる。ここでDES-Sを用いてトリプルDESと互換性のある暗号を構成しようとする場合を考える。DES-Sを3段重ねることでトリプルDESと互換性のある暗号を実現することは可能ではあるが、トリプルDES以上に効率が悪くなるという問題がある。

【0015】一方、DES、トリプルDES及びDES

-SSの何れもラウンド関数を利用し、同じ構造の処理を繰り返し行う積暗号と呼ばれる形式を用いている。このような形式の暗号は、上記した差分攻撃や線形攻撃に弱いという特徴を持っている。

【0016】本発明は、このような実情を考慮してなされたもので、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、単にDES-Sを3段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる暗復号装置及び記憶媒体を提供することを目的とする。

【0017】

【課題を解決するための手段】上記課題を解決するために、請求項1に対応する発明は、平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置であって、暗号処理又は復号処理を行う第1の暗復号化手段と、第1の暗復号化手段の出力を所定の置換表によりデータ置換する第1の置換手段と、第1の置換手段の出力に対し、暗号処理又は復号処理を行う第2の暗復号化手段と、第2の暗復号化手段の出力を所定の置換表によりデータ置換する第2の置換手段と、第2の置換手段の出力に対し、暗号処理又は復号処理を行う第3の暗復号化手段とを備えた暗復号装置である。

【0018】本発明はこのような手段を設けたので、各暗復号化手段の内容及び各置換手段の使用有無を調整することで、DES、トリプルDES、DES-Sのすべてと互換な単一の暗号アルゴリズムを構成するが、単にDES-Sを3段重ねるより効率がよいものとしてすることができる。また、置換手段によりデータ置換を行えば、データの連続性に擾乱が与えられるので、差分攻撃や線形攻撃にも強いアルゴリズムとすることができる。

【0019】次に、請求項2に対応する発明は、請求項1に対応する発明において、第1の暗復号化手段と第3の暗復号化手段、並びに、第1の置換手段と第2の置換手段は、それぞれ同一のアルゴリズムに従う手段となる暗復号装置である。

【0020】本発明はこのような手段を設けたので、より簡単な構成で請求項1に係る発明と同様な効果を得ることができる。

【0021】次に、請求項3に対応する発明は、請求項1又は2に対応する発明において、第1、第2及び第3の暗復号化手段並びに第1及び第2の置換手段それぞれに与える中間鍵を生成する鍵生成手段を備えるとともに、第1及び第2の置換手段は、鍵生成手段が生成した中間鍵に所定の情報が含まれているときには恒等変換として機能する暗復号装置である。

【0022】本発明はこのような手段を設けたので、第1及び第2の置換手段に与える中間鍵の内容を制御することで、DES、トリプルDES等の互換モードとそれ以外の強化暗号モードを容易に切り換えることができる。

【0023】次に、請求項4に対応する発明は、請求項3に対応する発明において、第1及び又は第3の暗号復号化手段は、鍵生成手段が生成した中間鍵に所定の情報が含まれているときには、第2の暗号復号化手段と同一のアルゴリズムに従う手段となる暗復号装置である。

【0024】本発明はこのような手段を設けたので、第1～第3の暗復号化手段に与える中間鍵の内容を制御することで、DES、トリプルDES等の互換モードにおける各モード切替を容易に行うことができる。

【0025】次に、請求項5に対応する発明は、請求項3又は4に対応する発明において、第2の暗復号化手段は、第1及び第3の暗号復号化手段が暗号化処理を行うときには復号処理を実行し、第1及び第3の暗号復号化手段が復号処理を行うときには暗号化処理を実行する暗復号装置である。

【0026】本発明はこのような手段を設けたので、容易にトリプルDESやDES、DES-SS間の切り替えを行うことができる。

【0027】次に、請求項6に対応する発明は、請求項5に対応する発明において、鍵生成手段は、第1及び第3の暗号復号化手段に同一の中間鍵を与える暗復号装置である。

【0028】本発明はこのような手段を設けたので、容易にトリプルDESを実現することができる。

【0029】次に、請求項7に対応する発明は、請求項5に対応する発明において、鍵生成手段は、第1及び第2の暗号復号化手段、又は、第2及び第3の暗号復号化手段が同一アルゴリズムとなりかつ同一暗復号鍵を使用する結果となる中間鍵を与える暗復号装置である。

【0030】本発明はこのような手段を設けたので、容易にDESやDES-SSを実現することができる。

【0031】次に、請求項8に対応する発明は、請求項1に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0032】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項1の暗復号装置として機能する。

【0033】次に、請求項9に対応する発明は、請求項6に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0034】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項3の暗復号装置として機能する。

【0035】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

（発明の第1の実施の形態）図1は本発明の第1の実施形態に係る暗復号装置の一例を示す構成図である。

【0036】この暗復号装置10は、第1、第2、第3暗復号化部11、13、15、第1、第2置換処理部1

2、14並びに鍵スケジュール部16を備える他、各機能部11～16を制御する制御部（図示せず）を備えて、暗号化装置、復号装置あるいは暗号化・復号装置として構成される。

【0037】ここで、平文21を第1暗復号化部11に入力し、第1置換処理部12、第2暗復号化部13、第2置換処理部14、第3暗復号化部15と処理を進めて暗号文22を出力する場合には暗号装置として機能し、暗号文22を第3暗復号化部15に入力し、上記と逆方向に処理を進める場合には復号装置として機能する。この何れの装置として、機能させるかは制御部の処理によって決まることになる。

【0038】また、暗復号装置10は、ハードウェア的にはCPUやメモリ等の計算機要素から構成されるものである。各機能部11～16はこの計算機要素が所定のプログラムに制御されて実現される。すなわち機能部11～16はハードウェア資源とソフトウェア資源の結合たる機能実現手段である。また、上記計算機要素及びプログラムは、パーソナルコンピュータやワークステーション等の計算機に提供されるものを使用するか、専用のチップを作成することにより、本暗復号装置10用に確保される。

【0039】次に、上記各機能部11～16の構成について説明する。

【0040】まず、鍵スケジュール部16は、外部から入力された鍵情報Kをもとに中間鍵に展開し、機能部11～15からなるデータ攪拌部に供給する。

【0041】機能部11～15からなるデータ攪拌部は、64ビット入力の平文21又は暗号文22を、鍵スケジュール部16からの鍵により攪拌して暗号化しあるいは復号し、対応する暗号文22若しくは平文21として出力する。

【0042】ここで、第1暗復号部11は、DES-SSのデータ攪拌部と同様な構成を備え、平文21を入力され、鍵スケジュール部16から入力された中間鍵の制御下で暗号化処理としての攪拌処理を行い、出力を第1置換処理部12に入力する。逆に、第1置換処理部12からの入力を鍵スケジュール部16からの中間鍵で復号し、平文21として出力する。なお、復号処理については、ここで説明したように暗号化処理の逆の処理を行うだけなので、以下の機能部12～15の説明においては暗号化を行う場合についてのみ説明し、特に断らない限り復号については省略する。

【0043】また、この第1暗復号部11は、DES-SSの構成を有することから、鍵スケジュール部16からの中間鍵の内容が一定の場合には単なるDESとして機能する。なお、DES-SSについては第2の実施形態で詳しく説明する。

【0044】第1置換処理部12は、第1暗復号処理部11から入力されたデータについて、中間鍵及び置換表

を用いたデータの置換処理を行い、その出力を第2暗復号化部13に inputs。また、中間鍵が一定の場合にはこの第1置換処理部12を未使用状態にできるようにになっている。未使用状態の場合は入力データをそのまま出力する。ここで、置換表は、乱数によって生成する方法若しくは代数的に生成する方法(式を用いる方法)によって作成される。何れの場合も差分確率及び線形確率の低い、すなわち差分攻撃や線形攻撃に強い置換表を作成する。

【0045】図2は置換処理部等に用いられる差分確率及び線形確率の低い置換表の一例を示す図である。

【0046】このような表は、差分確率及び線形確率の良好(低く)にできる代数式(例えば有限体GF(2⁸)上で原始多項式(x⁸+x⁴+x³+x²+1)を用いてx⁻¹(-1)を計算する; “[^]”は冪乗演算)を用いるか、差分確率及び線形確率が良くなるまで乱数計算を繰り返して作成する。

【0047】なお、本実施形態において差分確率及び線形確率が良好であるためには、それぞれの確率が理想値の2倍以下であることが望ましい。ここで8ビットの場合であれば、差分確率の理想値は4/256であり、線形確率の理想値は16/256である。

【0048】次に第2暗復号化部13は、DESのデータ攪拌部と同様な構成を備え、第1置換処理部12からの出力に対し、鍵スケジュール部16からの中間鍵の制御下で攪拌処理を行い、その出力を第2置換処理部14に inputs。なお、ここにおける攪拌処理は暗号文22を生成するための復号処理である。逆に平文21に復号するためには暗号処理がなされる。

【0049】第2置換処理部14は、第1置換処理部13と同様な構成を備え、中間鍵および置換表を用いたデータの置換処理を行い、出力を第3暗復号化部15に inputs。また、中間鍵が一定の場合には第2置換処理部14を未使用状態、すなわち入力と出力が一致するようになっている。

【0050】第3暗復号部15は、DES-SSのデータ攪拌部と同様な構成を備え、鍵スケジュール部16から入力された中間鍵の制御下で暗号化処理としての攪拌処理を行い、暗号文22を出力する。また、第3暗復号部15もDES-SSの構成を有するので、鍵スケジュール部16からの中間鍵の内容が一定の場合には単なるDESとして機能する。

【0051】次に、以上のように構成された本実施形態における暗復号装置の動作について説明する。

【0052】この暗復号装置においては、鍵スケジュール部16からの中間鍵により、第1、第3暗復号処理部11、15を、“DES”、“DES-SS”の何れか、また第1、第2置換処理部12、14を、“使用”、“未使用”の何れかの状態に選択できるようにになっている。これにより各機能部11~15の状態組み合

わせを適宜に変更可能である。

【0053】図3は各機能部の状態組み合わせの例を示す図である。

【0054】同図において、まず、第1、第3暗復号化部11、15をDESモードにし、第1、第2置換処理部12、14を未使用の状態にするとともに、第1、第2暗復号化部11、13に使用する鍵を同一にすると、暗復号装置全体はDESによる暗復号装置となる。

【0055】これは、第2暗復号化部13が平文21の暗号化に際して復号処理を行うため、第1暗復号処理部11で暗号化されたデータが第2暗復号化部13によって元の平文21に戻ってしまうためである。

【0056】次に、第1、第2、第3暗復号化部11、13、15をDESモードにし、第1、第2置換処理部12、14を未使用状態とすると、トリプルDESと同一の状態になる。トリプルDESは、平文を第1の鍵で暗号化し、その出力を第2の鍵で復号し、さらにその出力を第1の鍵で暗号化する方式である。ここでは、第1暗復号化部11が上記最初の暗号化を担当し、第2暗復号化部13が次の復号を担当し、第3暗復号化部15が最後の暗号化を担当する。

【0057】次に、第1暗復号化部11をDESモードにし、第1、第2置換処理部12、14を未使用状態とするとともに、第1、第2暗復号化部11、13に同一の鍵を使用するとDES-SSモードと同一の状態になる。上記の場合と同様に、第1、第2暗復号化部11、13の処理は互いにうち消し合って、平文21が第3暗復号化部15に inputsされる状態になるためである。

【0058】以上が本実施形態の暗復号装置10の有するDES、トリプルDES、DES-SS互換モードである。

【0059】次に、第1、第2置換処理部12、14を使用する場合には、上記互換モードよりも強化された暗号化を行うモードとなる。以下に説明する各場合は、第1、第2置換処理部12、14を使用するものである。

【0060】例えば第1、第2、第3暗号化部11、13、15すべてをオリジナルのモード(DES-SS、DES、DES-SS)で使った場合(図3:パターン1)、トリプルDESとDES-SSを組み合わせ、さらに各処理間に置換表による攪拌を加えたものとなる。

【0061】この場合、DES方式に類するラウンド関数の繰り返しによるデータ攪拌がDES-SSの長い鍵で十分に行われるとともに、各処理間で差分確率及び線形確率の低い置換表による攪拌が加えられるので、データの連続性に擾乱がおこり、線形攻撃や差分攻撃といった攻撃に対する防御力が強くなる。

【0062】また、第1、第3暗復号化部11、15をDESとし(図3:パターン2)、線形攻撃等からの防御力を保持しつつ、パターン1に比べて暗号化時間の短

縮化を図るようにすることも可能である。

【0063】さらに、第1、第3暗復号化部11、15の一方をDESとし、他方をDES-SSとしてパターン1とパターン2の中間的な暗号とすることも可能である。

【0064】また、上記各パターンの場合に、各暗復号化部11、13、15に与える鍵の組み合わせを変更して更に種々の暗号形式とすることができる。例えば暗復号化部11、13、15すべてに異なる鍵を与える、暗復号化部11、13に同一の鍵を与える、暗復号化部11、15に同一の鍵を与える、暗復号化部13、15に同一の鍵を与える、等のパターンが考えられる。

【0065】これらは、暗復号化装置10の処理能力や、互換モード及び強化暗号モードにおける各パターンの普及度等を考慮して適宜選択される。

【0066】上述したように、本発明の実施の形態に係る暗復号装置は、第1、第2、第3暗復号化部11、13、15を設け、各処理部の動作モード及び与える鍵を適宜変更できるようにしたので、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、DES-SSを3段重ねるより効率のよい暗号アルゴリズムの装置として構成することができる。したがって、このような暗号アルゴリズムの装置では独立して3つの暗号装置を持つよりも、装置規模を小さくすることができる。

【0067】また、本実施形態の暗復号装置10は、置換処理部12、14によって、データの連続性に擾乱を起こすことができるので、線形攻撃や差分攻撃等の同一構成の繰返しに着目した攻撃をより困難にすることができ、安全性を向上させることができる。

【0068】また、本実施形態の装置では、単一のアルゴリズムで種々の暗号方式を提供できるので、各暗号の普及度やハードウェアの処理能力の変化に応じて使用する暗号方式を選択することができ、長期間に渡って使用することができる。

(発明の第2の実施の形態) 本実施形態では、第1の実施形態における各機能部11~16の構成をより具体化させた場合について説明する。したがって、本実施形態は第1の実施形態と同様に構成される他、各機能部11~16における更なる形態例が示されるものである。

【0069】本実施形態の暗復号装置10は、図1に示す第1の実施形態の暗復号装置と同様に構成されている。以下、各機能部11~16の構成例を説明する。なお、本実施形態の各図面においては、第1実施形態の図1と同一部分には同一符号を付して詳細説明を省略する。

〔鍵スケジュール部16の構成動作〕まず、鍵スケジュール部16について説明する。

【0070】図4は鍵スケジュール部の全体構成を示す

図である。

【0071】同図に示すように、鍵スケジュール部16には、256ビットの鍵情報Kを5つに分割し各レジスタ32、33、34、35、36に格納する分割部31と、レジスタ32~35から56ビットの鍵情報を読み出しこれを拡大転置して64ビットにする拡大転置部37とが設けられている。さらに、拡大転置結果若しくはレジスタ36の内容から中間鍵K1、K2、K3並びにKK1及びKK2をそれぞれ生成するDES-SS鍵スケジュール部38、39、DES鍵スケジュール部40及び置換用鍵スケジュール部41が設けられ、鍵スケジュール部16が構成されている。

【0072】ここで256ビットの鍵情報は、分割部31において56ビットからなる4つのブロックB1、B2、B3、B4と、32ビットの1つのブロックB5に分割され、それぞれレジスタ32~36に記憶される。この場合の分割の仕方は、256ビットを先頭から順次56ビットずつ切り出してそれぞれB1~B4とし、さらに最後の残り32ビットをB5とするものである。

【0073】また、ブロックB1からブロックB4までの4つのブロックはそれぞれ拡大転置部37に入力され、それぞれ拡大転置表によって64ビットに拡大される。

【0074】図5は拡大転置表の一例を示す図である。

【0075】同図の表は先頭から出力ビットに対応しており、また各出力ビットにおける数字は入力が第nビット目であるかをあらわす。ただし、表中の0はその出力ビットとして0が出力されることを表す。

【0076】次に、ブロックB1を拡大した64ビットの鍵とブロックB2を拡大した64ビットの鍵を連結した128ビットの鍵は、第1暗復号部11への中間鍵K1を出力するDES-SS鍵スケジュール部38に入力される。

【0077】また、ブロックB1を拡大した64ビットの鍵とブロックB3を拡大した64ビットの鍵を連結した128ビットの鍵は、第3暗復号部15への中間鍵K3を出力するDES-SS鍵スケジュール部39に入力される。

【0078】また、ブロックB4を拡大した64ビットの鍵は、第2暗復号部15への中間鍵K2を出力するDES鍵スケジュール部40に入力される。さらに、32ビットのブロックB5は拡大転置されることなく置換用鍵スケジュール部41に入力される。

【0079】上記各鍵スケジュール部38~41のうち、DES鍵スケジュール部40は一般的なDESにおける拡大鍵生成手段と同様な構成を有するのみであるので、詳細説明は省略し、以下、DES-SS鍵スケジュール部38、39及び置換用鍵スケジュール部41について説明する。

【0080】図6はDES-SS鍵スケジュール部の構

成例を示すブロック図である。

【0081】DES-SS鍵スケジュール部38, 39は、Aスケジュール部45, Bスケジュール部46及びFG拡大鍵生成部47から構成される。なお、FG拡大鍵生成部47は各ラウンド(1段~16段)に対応して設けられるとともに、Aスケジュール部45及びBスケジュール部46内も16段の構成となっており、同図にはそれぞれ第1段のみが示されている。なお、符号以外の同図における数値はビット数を現している。

【0082】拡大転置部37から入力される128ビットの鍵のうち、各ブロックB1, B2若しくはB3に対応する部分がそれぞれAスケジュール部45, Bスケジュール部46に入力されるようになっている。

【0083】Aスケジュール部45及びBスケジュール部46は、入力される鍵が異なり、また拡大鍵を生成するためのデータの出力の仕方が異なる点を除けば、一般的なDESにおける拡大鍵生成手段と同様な構成となっているので詳細説明は省略する。

【0084】ここで、DES-SS用とDES用の中間鍵における相違点は、DES-SSではDESの攪拌手段に使用されるF関数拡大鍵に加え、G関数拡大鍵が必要な点である。

【0085】図6におけるAスケジュール部45及びBスケジュール部46では、ビット選択部48A, 48Bが中間鍵K1/K2を生成するための情報を出力する。

【0086】ここでまず、Aスケジュール部45のビット選択部48Aは、F関数拡大鍵FK1を出力するとともに、5ビットの鍵A1を出力する。この5ビットの鍵A1は例えばビット選択部48Aに入力されてなる56ビットの鍵の左から9, 18, 22, 25, 35番目の5ビットが用いられる。この5ビット選択方法は他の方法でも良い。

【0087】一方、Bスケジュール部4のビット選択部48Bは、G関数拡大鍵の元になる48ビットの鍵GB1を出力するとともに、鍵A1と同様な5ビットの鍵B1を出力する。Aスケジュール部45及びBスケジュール部46が一般的なDESの拡大鍵生成手段と異なるのは、ビット選択部48A, 48B(以下の、2~16段も同様)の処理がこのように修正されている点のみである。

【0088】FG拡大鍵生成部47は、ビット選択部48Aが出力した鍵をそのままF関数拡大鍵FK1として出力する。また、48ビットの鍵GB1とF関数拡大鍵FK1の排他的論理和49をとってG関数拡大鍵GK1の一部(G1, G2, G3)として出力する。さらにFG拡大鍵生成部47は、鍵A1と鍵B1との間で排他的論理和50を取り、さらにその出力と0X10(0Xは16進を表す)との間で排他的論理和51をとってG関数拡大鍵GK1の一部(G4)として出力する。

【0089】こうして、DES-SS鍵スケジュール部

38, 39によって、F関数拡大鍵FK1と、鍵G1, G2, G3, G4からなるG関数拡大鍵GK1とを含む中間鍵K1, K3が得られる。

【0090】DES-SS鍵スケジュール部38が出力した中間鍵K1は第1暗復号化部11に入力され、DES-SS鍵スケジュール部39が出力した中間鍵K3は第3暗復号化部15に入力されることとなる。なお、詳細説明は省略したが、DES鍵スケジュール部40が出力した中間鍵K2は第2暗復号化部13に入力され、第2暗復号化部13によって、DESによる暗復号が実行される。

【0091】次に、置換用鍵スケジュール部41について説明する。

【0092】図7は置換用鍵スケジュール部の構成例を示すブロック図である。

【0093】この置換用鍵スケジュール部41は、レジスタ36のブロックB5を32ビットの鍵として入力し、第1置換処理部12に入力される中間鍵KK1と、第2置換処理部14に入力される中間鍵KK2を出力するものである。

【0094】まず、レジスタ54内の32ビットの鍵C0'は、そのまま第1置換処理部12用の中間鍵KD1(32ビット)として出力されるとともに、論理和部55及び左シフト部56に入力される。なお、レジスタ54はレジスタ36と同一であってもよい。

【0095】論理和部55では、32ビットの鍵C0'における各ビットの論理和が計算結果として出力され、第1置換処理部12用の中間鍵KS1(1ビット)となる。

【0096】この中間鍵KD1と中間鍵KS1とから中間鍵KK1が構成され、第1置換処理部12に入力される。

【0097】次に、左シフト部56に入力されたデータは同シフト部56により4ビットほど左シフトされた後、鍵C1としてレジスタ57に格納される。

【0098】この鍵C1'は、第2置換処理部14に入力される32ビットの中間鍵KD2となり、また、論理和部58において32ビットC1'の論理和の計算結果が、第2置換処理部14に入力される1ビットの中間鍵KS2となる。

【0099】この中間鍵KD2と中間鍵KS2とから中間鍵KK2が構成され、第2置換処理部14に入力される。

【0100】以上が鍵スケジュール部16の構成及び動作であり、次に、置換処理部12, 14について説明する。

[置換処理部12, 14の構成動作] 図8は置換処理部の構成例を示すブロック図である。

【0101】同図に示すように置換処理部12, 14は、初期転置部61と、排他的論理和62~66と、置

換部 67～74 と、逆転置部 75 とから構成されている。置換部 67～74 には、図 2 に示すような置換表が保持されており、入力を置換表により変換して出力する。

【0102】ここで、まず、暗復号化部からの 64 ビットの入力は、初期転置（初期転置 IP）部 61 においてビット転置が行われ、その結果が 8 ビットずつの 8 つのブロックに分割される。

【0103】初期転置 61 の出力のうち 8 ビットブロック 4 つからなる 32 ビットはそのまま置換部 67～70 10 に入力される。残りの 8 ビットブロック 4 つからなる 32 ビットは排他的論理和 62～66 において中間鍵 KD（中間鍵 KD1/KD2）との排他的論理和が行われ、その結果が置換部 71～74 に入力される。

【0104】置換部 67～74 には、8 ビットの入力データと 1 ビットの鍵 KS（中間鍵 KS1/KS2）とが入力される。ここで、鍵ビットが 1 の場合には、置換表を用いた入力に対応する出力データが出力され、鍵ビットが 0 の場合には、入力と同一の出力データが出力される。すなわち鍵 KS が 0 ビットの場合には置換処理部 1 20 2、14 は未使用状態となる。

【0105】各置換部 67～74 からの出力は逆転置（逆転置 IP⁻¹）75 に入力され、ここでビット転置が行われたのち、64 ビットデータとして出力される。

〔第 1、第 3 暗復号化部 11、15 の構成動作〕次に、DES-SS のデータ搅拌手段として構成される第 1、第 3 暗復号化部 11、15 について説明する。

【0106】図 9 は DES-SS として構成された暗復号化部の構成例を示すブロック図である。

【0107】DES-SS として構成された第 1、第 3 30 暗復号化部 11、15 は、鍵 GK 及び FK からなる中間鍵 K1 又は K3 に依存して入力（64 ビット）を搅拌し、対応する暗号文を出力する。この暗復号化部 11、15 は、初期転置部（初期転置 IP）80 と、第 1 段から第 16 段までのデータ搅拌部 81～96 と、最終転置部（最終転置 IP⁻¹）97 とから構成されている。各データ搅拌部 81～96 は、暗号化関数としての F 関数 81f～96f 及び排他的論理和 81a～96a を備えて DES のデータ搅拌手段と同様に構成される他、鍵 GK を用いてデータを搅拌する暗号化関数としての G 関数 8 40 1g～96g をも備えている。

【0108】ここで、F 関数 81f～96f は、通常の DES と同様な搅拌処理を行うものであり、中間鍵 K1、K3 のうちの F 関数拡大鍵 FK と G 関数 81g～96g の出力を受け、所定の搅拌処理を行ってその結果を排他的論理和 81a～96a に入力する。

【0109】排他的論理和 81a～96a は、32 ビットの Ln（L0～L15）と F 関数 81f～96f の出力との間の排他的論理和を次段の入力の右側 32 ビット Rn+1 として出力する。

【0110】また、G 関数 81g～96g は、後述する搅拌処理を行うものであり、中間鍵 K1、K3 のうちの G 関数拡大鍵 GK と Rn（R0～R15）を受け、所定の搅拌処理を行って次段の入力の左側 32 ビット Ln+1 及び F 関数 81f～96f へ出力する。

【0111】各段のデータ搅拌部 81～96 では同様な処理が実行される。まず第 1 段の動作について説明する。

【0112】暗復号化部 11、15 において、入力（64 ビット）は初期転置部 80 にて転置された後、2 つに等分割されて左側 32 ビット L0 と右側 32 ビット R0 として生成される。

【0113】第 1 段データ搅拌部 81 において、R0 は暗号化 G 関数 81g に入力され、その G 関数出力が暗号化 F 関数 81f に入力されるとともに、第 2 段データ搅拌部 82 に左側 32 ビット L1 として出力される。一方、L0 は排他的論理和部 81a に入力され、F 関数 81f との間で排他的論理和が取られた後、第 2 段データ搅拌部 82 に右側 32 ビット R1 として出力される。

【0114】以上の搅拌処理が第 1 段で行われたのち、以下、第 16 段まで第 1 段と同様な搅拌処理が行われる。第 16 段の出力は最終転置部 97 によって転置が行われた後、64 ビットの出力となる。

【0115】次に G 関数 81g～96g における処理について説明する。

【0116】図 10 は G 関数の構成例を示すブロック図である。

【0117】この G 関数 81g～96g は、入力データに対し、G 関数拡大鍵 GK に含まれる 4 つの鍵 G1、G2、G3、G4 を用いた搅拌を行ってデータ出力するのである。このために、G 関数 81g～96g は、排他的論理和部 103、104、108、論理積部 101、106、左シフト部 105 を備えている。

【0118】なお、同図に示す L0'、L1'、L2'、L3'、R0'、R1'、L2'、R3' は、これらのデータがレジスタに格納され、あるいは次の機能手段に引き渡されることを示す。

【0119】この G 関数においては、まず入力（32 ビット）は、2 つに等分割されて左側 32 ビット L0' と右側 32 ビット R0' が生成される。

【0120】R0' は論理積部 101 及び排他的論理和部 104 に入力され、L0' は排他的論理和部 103 に入力される。

【0121】論理積部 101 において R0' と拡大鍵 G1 の論理積が行われ、排他的論理和部 103 に出力される。排他的論理和 103 においては L0' と論理積部 101 の出力との排他的論理和が行われ、その結果 L1' が左シフト 105 に入力される。

【0122】一方、排他的論理和 104 においては R0' と拡大鍵 G2 との排他的論理和が行われ、その結果 50

R1' が左シフト部105に入力される。

【0123】左シフト部105においては、拡大鍵G4のビット数に従った左シフトが行われ、そのシフト結果の出力は2つに等分割して左側32ビットがR2'に、右側32ビットがL2'となる。

【0124】R2'は論理積部106に入力され、L2'は排他的論理和部108に入力される。論理積部106においてはR2'と拡大鍵G3の論理積が行われ、排他的論理和部108に出力される。

【0125】さらに、排他的論理和部108において、L2'と論理積部106の出力との排他的論理和が行われ、G関数の出力の左側32ビットとなる。一方、G関数の出力の右側32ビットはR2'が用いられる。

【0126】このG関数においては、入力を分割しその分割入力を再び接続してシフトしつつ、その間に攪拌処理を挿入して出力データの攪拌度合いを高いものにして

いる。
〔第2暗復号化部13の構成動作〕第2暗号化部13は、一般的なDESのデータ攪拌手段と同様に構成されているので、ここでは詳細な説明は省略する。なお、DESのデータ攪拌手段については（岡本栄司著、「暗号理論入門」、共立出版、1993）等に記載されている。また、例えば図9に示すDES-SSの構成からG関数81g～96gを取り除きG関数拡大鍵GKを不要としたものは、DESのデータ攪拌手段の一例となっている。

〔鍵情報Kに対応した暗復号装置10の動作〕本実施形態の暗復号装置10の各機能部11～16が上記したように構成され動作するときに、鍵スケジュール部16に与える鍵情報Kの内容により、暗復号装置10がいかなる内容の暗号若しくは復号装置となるかについて説明する。

【0127】ここで、鍵情報Kは、図4に示すように、ブロックB1～B5に分割されるものであり、各ブロックB1～B5の内容がどのようにになっているかにより本装置10における処理が決まることになる。

【0128】まず、ブロックB5の部分に少なくともビットが立っており、その論理和55、58が0にならない場合には、鍵KSが0とならずひいては図8に示す置換処理部12、14における置換部67～74において置換処理が実行される。この場合には、暗復号装置10は、図3における強化暗号モードとして動作する。この結果、従来のDES、DES-SS又はトリプルDESとは異なり、置換表による暗号連続性が擾乱された暗号となって、より強化された暗号化が実現される。

【0129】特に、ブロックB1からブロックB5の鍵情報として独立したものを与えれば、より安全性の高い256ビット鍵の暗号化アルゴリズムとして使用される。

【0130】一方、置換用鍵スケジュール部41に入力

される32ビットの鍵ブロックB5の入力ビットがすべて0である場合には論理和55、58の出力である鍵KSが0になるため、置換処理部12及び14における置換表が使用されない。したがって、この場合の中間鍵KK1、KK2によっては、置換処理部12及び14において、入力と同一のデータが出力され恒等変換が行われることになる。

【0131】置換処理部12及び14にて恒等変換が行われる場合には、暗復号装置10は図3における互換モードとして動作することになる。以下、この場合について、更に具体的に説明する。

【0132】まず、図4において、ブロックB1と同一の内容をブロックB2及びB3に入力することにより、DES-SS鍵スケジュール部38及び39は、第1、第3暗復号化部11、15がDES暗号化モードとなる暗号化処理を行う中間鍵を生成する。第1、第3暗復号化部11、15がDESモードになるためには、図9におけるG関数入出力が恒等変換となればよい。この恒等変換は、図10に示すG関数処理において、拡大鍵G1～G4が所定の入力になれば実現される。

【0133】このとき、暗号化装置全体としては、ブロックB1に入力された鍵ビットによる第1暗復号化部11のDES暗号化と、ブロックB4に入力された鍵ビットによる第2暗復号化部13のDES復号の処理となり、56ビットからなる2つの鍵を用いたトリプルDESと同一の処理内容となる。

【0134】この場合に、さらにブロックB1とブロックB4に同一の内容を用い、ブロックB2とB3のいずれか一方をブロックB1と同一の内容に設定することにより、DES-SSとの互換モードとして動作する。これは、ブロックB1と同一内容を入力する側の暗復号化部11又は15がDESモードで動作して、第2暗復号化部13の処理とキャンセルするため、結果としてDES-SSモードの部分のみが残るからである。

【0135】このとき、例えばブロックB3をブロックB1と同一の内容とすると、暗号化装置10全体としては、ブロックB1とB2をそれぞれ拡大転置した出力を結合した128ビットの鍵を入力とするDES-SSと同一の処理内容となる。

【0136】上述したように、本発明の実施の形態に係る暗復号装置は、256ビットの鍵情報Kを5つのブロックに分割し、各ブロック情報を用いて実質的な中間鍵情報のみならず、第1、第2置換処理部12、14の使用有無、及び、第1、第2、第3暗復号化部11、13、15の動作モード指定ができる情報を生成し、これによって装置全体の動作モードを制御するようにしたので、第1の実施形態と同様な装置を実現させ、その作用効果を得ることができる。

【0137】すなわち本実施形態では、鍵情報Kの内容を修正するだけで動作モードの変更を容易に行うことが

でき、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するとともに、データの連続性に擾乱を起せる線形攻撃や差分攻撃等に強い暗号をも実現させることができる。

(発明の第3の実施形態) 本実施形態は、第2の実施形態における第1、第3暗復号化部11、15のG関数に改良を加えた場合について説明する。

【0138】図11は本発明の第3の実施形態に係る暗復号装置におけるG関数の構成例を示すブロック図であり、図1～図10と同一部分には同一符号を付して説明を省略する。

【0139】この暗復号装置10は、図11に示すように、第1、第3暗復号化部11、15のG関数81g～96gにおいて、論理積101～排他的論理和103間に置換部102、論理積106～排他的論理和108間に置換部107が挿入される他、第2の実施形態と同様に構成されている。したがって、本実施形態にて説明するG関数81g～96gは厳密にはDES-SSのG関数とは異なるものであり、DES-SS用のG関数が修正されたものである。

【0140】置換部102、107は、差分の線形性および非線形性の高い特性を有する、例えば図2に示すような置換表を保持しており、入力を置換表により変換して出力する。

【0141】このように構成された本実施形態の暗復号装置10は第2の実施形態と同様に動作する他、新たな付加された置換部102、107部分については以下のように動作する。

【0142】まず、置換部102においては、論理積101の出力が入力されるようになっている。この論理積出力は置換表にて置換され、その結果が排他的論理和103に出力される。

【0143】また、置換部107においては、論理積106の出力が入力されるようになっている。この論理積出力は、置換部102の場合と同様に置換表にて置換され、その結果が排他的論理和108に出力される。

【0144】本実施形態のG関数81g～96gでは、その中に差分確率及び線形確率が低い置換表による置換102、107が挿入されているために、データの連続性に擾乱が起これ、線形攻撃や差分攻撃に強い暗号化が実現されている。

【0145】この置換部102、107に用いる置換表として、本実施形態では図2に示す表を用いると説明したが、この変形例として図2の置換表をアフィン変換して入力0に対する出力が0である置換表を用いることも考えられる。このとき、特定の鍵入力の場合には置換部102、107の出力が0となり、排他的論理和部103及び108における鍵情報の挿入が行われなくなる。したがって、このような置換表を用いた場合には、G関数は入力と出力が一致する恒等変換の関数として機能す

ることも可能になる。

【0146】上記置換部102、107を用いることにより、論理積部101及び106における鍵との論理積の結果、論理積の出力ビットの0ビットと1ビットの出現率に不均一性が現れても、置換部102、107の処理により、この不均一性を是正し、鍵に含まれる1ビットの数に着目した攻撃に対して安全になる。

【0147】例えば拡大鍵G1に出現する1ビットの数が1個の場合には、排他的論理和部103においてさされる鍵、すなわち排他的論理和が行われる実質ビット数は高々1ビットである。しかし、置換部102による置換の結果、さされる鍵のビット数は変化し、鍵に含まれる1ビットの数に着目した攻撃に対して安全になる。

【0148】上述したように、本発明の実施の形態に係る暗復号装置は、G関数に置換部102、107を挿入したので、データの連続性に擾乱が起これ、線形攻撃や差分攻撃に強い暗号化を実現することができる。

【0149】なお、実施形態に説明した装置は、記憶媒体に格納したプログラムをコンピュータに読み込ませることで実現させることができる。

【0150】ここで本発明における記憶媒体としては、磁気ディスク、フロッピー（登録商標）ディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD等）、光磁気ディスク（MO等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【0151】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【0152】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【0153】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。

【0154】なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【0155】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0156】

【発明の効果】以上詳記したように本発明によれば、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、単にDES-SSを3段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる暗復号装置及び記憶媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る暗復号装置の一例を示す構成図。

【図2】置換処理部等に用いられる差分確率及び線形確率の低い置換表の一例を示す図。

【図3】各機能部の状態組み合わせの例を示す図。

【図4】鍵スケジュール部の全体構成を示す図。

【図5】拡大転置表の一例を示す図。

【図6】DES-SS鍵スケジュール部の構成例を示すブロック図。

【図7】置換用鍵スケジュール部の構成例を示すブロック図。

【図8】置換処理部の構成例を示すブロック図。

【図9】DES-SSとして構成された暗復号化部の構成例を示すブロック図。

【図10】G関数の構成例を示すブロック図。

【図11】本発明の第3の実施形態に係る暗復号装置におけるG関数の構成例を示すブロック図。

【符号の説明】

- 10…暗復号装置
- 11…第1暗復号化部
- 12…第1置換処理部
- 13…第2暗復号化部
- 14…第2置換処理部
- 15…第3暗復号化部
- 16…鍵スケジュール部
- 21…平文
- 22…暗号文

* 31…分割部

37…拡大転置部

38, 39…DES-SS鍵スケジュール部

40…DES鍵スケジュール部

41…置換用鍵スケジュール部

45…Aスケジュール部

46…Bスケジュール部

47…FG拡大鍵生成部

48A, 48B…ビット選択部

10 49, 50…排他的論理和

55, 58…論理和部

56…左シフト部

61…初期転置部

62~66…排他的論理和

67~74…置換部

75…逆転置部

80…初期転置部

81~96…データ攪拌部

81a~96a…排他的論理和

20 81f~96f…F関数

81g~96g…G関数

97…最終転置部

101, 106…論理積部

102, 107…置換部

103, 104, 108…排他的論理和部

105…左シフト部

B1~B4…ブロック

FK…F関数拡大鍵

G1~G4…拡大鍵

30 GK…G関数拡大鍵

K1…第1暗復号化部への中間鍵

K2…第2暗復号化部への中間鍵

K3…第3暗復号化部への中間鍵

KK1…第1置換処理部への中間鍵

* KK2…第2置換処理部への中間鍵

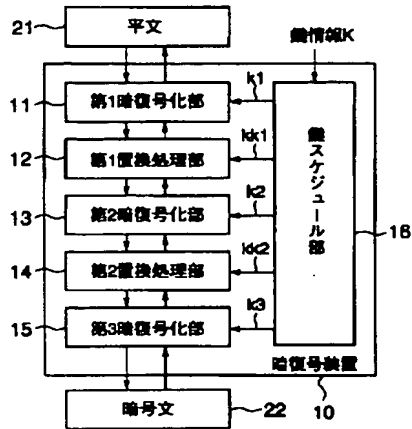
【図2】

置換表															
0	1142	244	71	187	122	188	173	157	221	152	61	170	93	150	
1	118	114	179	89	223	82	76	103	144	222	85	128	180	131	75
2	137	111	48	184	186	84	84	80	34	207	168	171	12	21	223
3	54	85	248	213	148	78	166	4	48	138	43	30	22	103	68
4	56	35	104	140	128	28	37	87	18	193	203	88	151	14	59
5	38	87	202	91	188	198	23	77	82	141	238	109	30	23	49
6	40	209	17	217	233	251	218	121	219	119	6	187	130	20	250
7	27	84	181	28	124	204	228	176	73	48	38	45	83	105	2
8	24	223	68	78	152	183	15	82	11	220	189	148	172	108	2245
9	28	130	158	188	155	183	15	82	11	220	189	148	172	108	2245
10	135	228	238	107	235	242	181	175	187	100	7	123	46	154	189
11	16	88	185	33	101	184	183	158	210	247	88	90	33	124	188
12	41	113	200	248	249	87	213	314	16	115	118	120	153	10	25
13	20	63	230	240	134	177	228	241	250	118	243	180	108	30	178
14	227	231	181	234	3	143	211	201	66	212	232	117	127	255	126

【図5】

拡大転置表															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
18	30	0	17	18	19	0	20	21	0	22	23	24	25	26	27
42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	

【図1】



【図3】

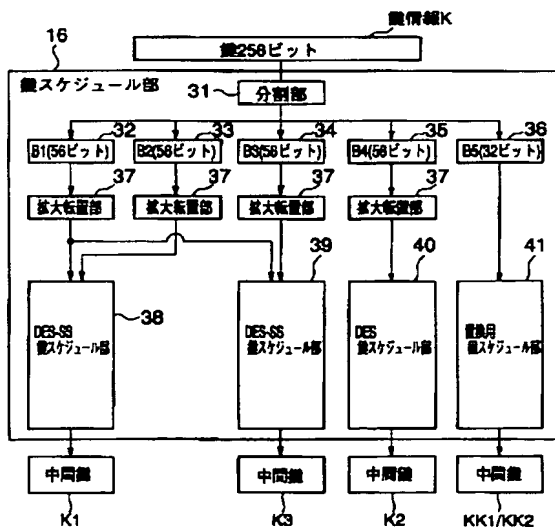
	互換モード			強化暗号モード		
第1暗号化部	DES	DES	DES	DES-SS	DES	
第1置換処理部	未使用	未使用	未使用	使用	使用	
第2暗号化部	DES	DES	DES	DES	DES	...
第2置換処理部	未使用	未使用	未使用	使用	使用	
第3暗号化部	DES	DES	DES-SS	DES-SS	DES	
得られる暗号	DES *1	トリプルDES *2	DES-SS *3	パターン1	パターン2	...

*1: 第1、第2暗号化部で同一の鍵を使用する

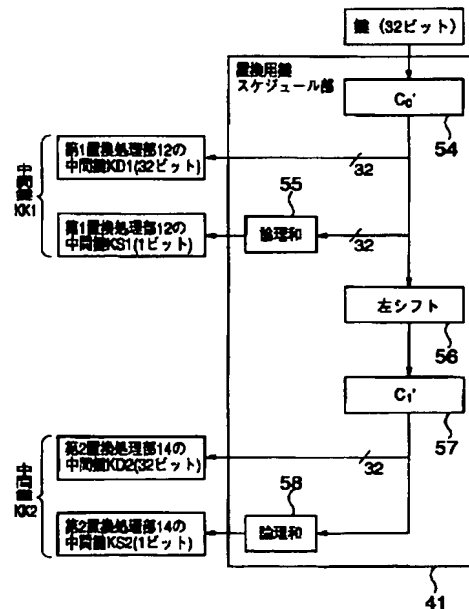
*2: 第1、第3暗号化部で同一の鍵、第2暗号化部で異なる鍵を使用する

*3: 第1、第2暗号化部で同一の鍵を使用する

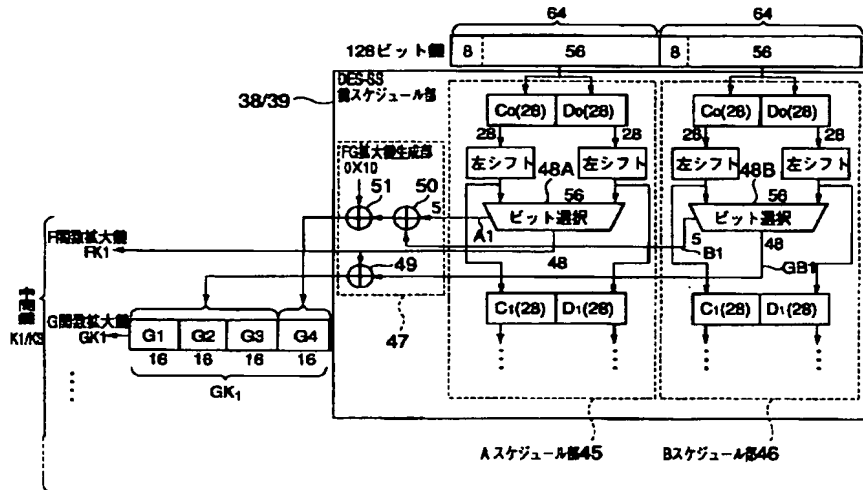
【図4】



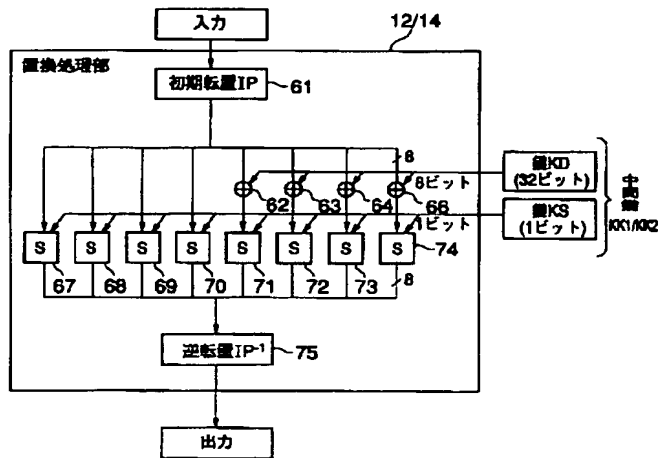
【図7】



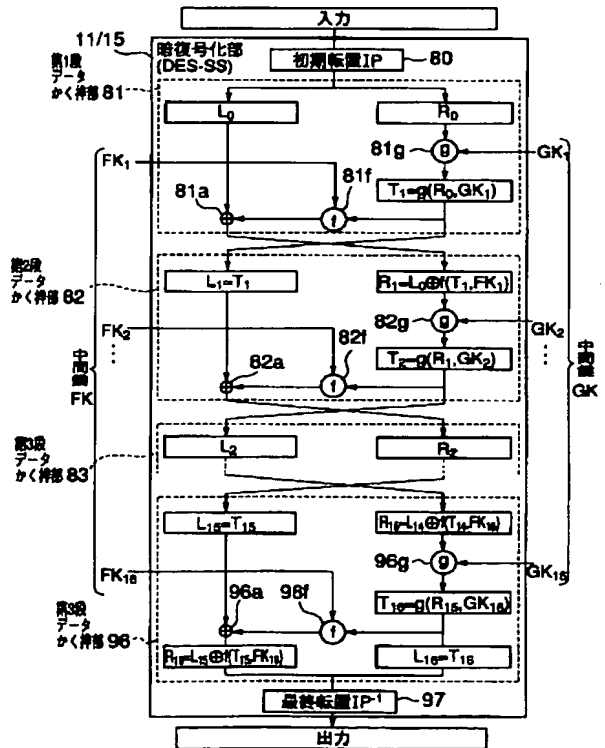
【図6】



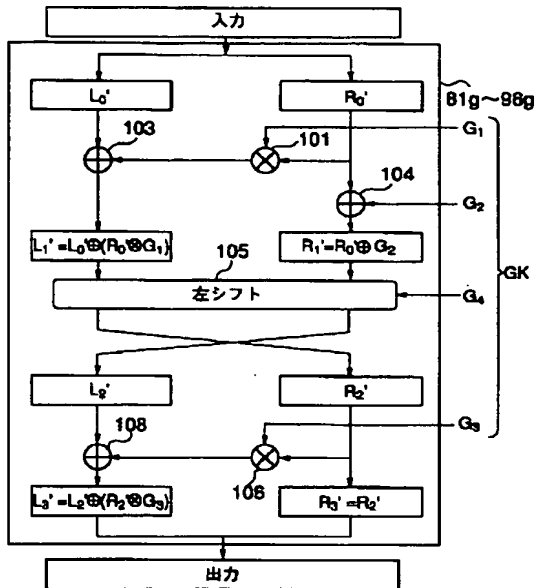
【図8】



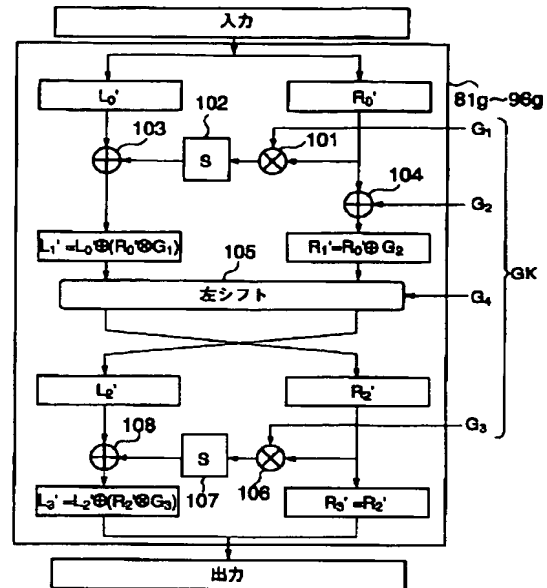
【図9】



【図 10】



【図 11】



フロントページの続き

(72) 発明者 清水 秀夫
東京都府中市東芝町 1 番地 株式会社東芝
府中工場内

F ターム (参考) 5J104 AA18 AA41 JA15 NA02 NA09
NA27 PA07